UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,931	12/15/2003	Steven Tischer	030515 (BLL-0144)	3718

36192 7590 07/20/2009

AT&T Legal Department - CC
Attn: Patent Docketing
Room 2A-207
One AT&T Way
Bedminster, NJ 07921

EXAMINER	
HAILE, AWET A	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
07/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/735,931
Filing Date: December 15, 2003
Appellant(s): TISCHER, STEVEN

____
David A. Fox

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 04/22/2009 appealing from the Office action mailed 10/17/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct

(8) Evidence Relied Upon

US 5742684 A	Labaton et al	04-1998
US 20030191949 A1	Odagawa	10-2003
US 20020004903 A1	Kamperman et al	01-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections – 35 USC§ 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. **Claims 1-4, 6,7,11-15, 17, 18 and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton et al (US 5742684) in view of Odagawa (US 2003/0191949 A1).

Regarding claim 1, Labaton '684 discloses, a method for transmitting data over a computer network to a predetermined recipient (see Fig 1, i.e. transmitting bank card information from special tone dialer(STD) unit 16 to the host computer 28), the method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message(see column 5, lines 10-13, i.e. the card information is encrypted using the current time(GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter(see column 5, lines 10-13, i.e. Greenwich Mean Time(GMT));

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (see column 6, lines 59-67, i.e. encrypting the next message using the changing GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (see column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

transmitting the first and second modified data messages to a first device(see Fig.1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28);determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving interface computer 26 in order to use it as a decryption key);

and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (see column 6, line 60 - column 7 line 5, i.e. the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute using the same encryption key (GMT));

Labaton ’684 does not explicitly teach, wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

Odagawa ‘949 teaches, wherein the first message modification key value being determined based on the at least one variable parameter (see paragraphs 126, 204, Figs. 2 and 7, i.e. using variable information from a variable information provider 47 to generate encryption key 43) and a unique identifier identifying the predetermined recipient(see paragraphs 205-207, 210, Figs. 2 and 7, i.e. information receiver 61 receiving , encrypted information 66, which is encrypted using variable information from variable information provider and biometrics information from a receiving user), the unique identifier being a biometric identifier obtained from the recipient(see paragraphs, 205, 210 and Fig. 2, i.e. a biometric information from a service receiving user is used to generate encryption keys).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using variable information and biometrics information for generating an encryption key as taught by Odagawa ‘949, into the communication system of Labaton ’684, in order to ensure that abuse of a service medium by a third party is more surely prevented, since such method is suggested by Odagawa ‘949(see paragraph 205).

Regarding claim 2, Labaton’684 discloses, wherein the variable parameter comprises a time- varying parameter (column 6, line 60-67, i.e. changing the encryption algorithm periodically).

Regarding claim 3, Labaton'684 discloses, wherein the time-varying parameter includes at least one of a determined hour, minute, and second (see column 5 lines 10-12, i.e. GMT is used as an encryption key).

Regarding claim 4, Labaton'684 failed to teach, recipient biometric identifier obtained from the recipient is a voice sample of the recipient.

However, Odagawa '949 teaches, recipient biometric identifier obtained from the recipient is a voice sample of the recipient (see paragraphs 91 and 92, i.e. voice print from a service receiving user is used as a biometrics information to generate encryption key)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using variable information and biometrics information for generating an encryption key as taught by Odagawa '949, into the communication system of Labaton '684, in order to ensure that abuse of a service medium by a third party is more surely prevented, since such method is suggested by Odagawa '949(see paragraph 205).

Regarding claim 6, Labaton'684 discloses, transmitting the first and second message modification key values to a first computer(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key).

Regarding claim 7, Labaton'684 discloses, wherein the first and second modified data messages are both transmitted via a first communication channel (see Fig.1, transmission line 24, i.e. the encrypted data is transmitted via transmission line 24).

Regarding claim 11, Labaton'684 discloses, a system for transmitting data over a computer network to a predetermined recipient (see Fig. 1, i.e. transmitting bank card information from special tone dialer unit 16 to the host computer 28), the system comprising:

a first device configured to modify at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message (see column 5, lines 10-13, notice, the card information is encrypted using the current time (GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter (see column 5, lines 10-13, Greenwich Mean Time (GMT));

the first device further configured to modify at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (see column 6, lines 59-67, encrypting the next message using different GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (see column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

the first device configured to transmit the first and second modified data messages(see Fig 1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28); and a second device configured to receive the transmitted first and second modified data messages and to determine the first data message for the predetermined recipient based on the modified first data message and the first message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key);

the second device further configured to determine the second data message for the predetermined recipient based on the modified second data message and the second message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the first device is configured to modify multiple bytes of a first data message by adding the first message modification key byte value to multiple bytes of the first data message (see column 6, line 60 - column 7 line 5, notice, the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute with the same encryption key (GMT));

Labaton ’684 does not explicitly teach, wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

Odagawa ‘949 teaches, wherein the first message modification key value being determined based on the at least one variable parameter (see paragraphs 126, 204, Figs. 2 and 7, i.e. using variable information from a variable information provider 47 to generate encryption key 43) and a unique identifier identifying the predetermined recipient(see paragraphs 205-207, 210, Figs. 2 and 7, i.e. information receiver 61 receiving , encrypted information 66, which is encrypted using variable information from variable information provider and biometrics information from a receiving user), the unique identifier being a biometric identifier obtained from the recipient(see paragraphs, 205, 210 and Fig. 2, i.e. a biometric information from a service receiving user is used to generate encryption keys).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using variable information and biometrics information for generating an encryption key as taught by Odagawa ‘949, into the communication system of Labaton ’684, in order to ensure that abuse of a service medium by a third party is more surely prevented, since such method is suggested by Odagawa ‘949(see paragraph 205).

Regarding claim 12, Labaton’684 discloses, wherein the first and second devices comprise first (see Fig 1, i.e. STD 16) and second computers (see Fig 1, i.e. interface computer

26), respectively, operatively communicating with one another (Fig 1, STD 16 and interface computer 26 connected to each other).

Regarding claim 13, Labaton'684 discloses, wherein the variable parameter comprises a time- varying parameter (see column 6, line 60-67, i.e. changing the encryption algorithm periodically).

Regarding claim 14, Labaton'684 discloses, wherein the time-varying parameter includes at least one of a determined hour, minute, and second (see column 5, lines 10-12, i.e. GMT is used as an encryption key).

Regarding claim 15, Labaton'684 failed to teach, recipient biometric identifier obtained from the recipient is a voice sample of the recipient.

However, Odagawa '949 teaches, recipient biometric identifier obtained from the recipient is a voice sample of the recipient (see paragraphs 91 and 92, i.e. voice print from a service receiving user is used as a biometrics information to generate encryption key)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using variable information and biometrics information for generating an encryption key as taught by Odagawa '949, into the communication system of Labaton '684, in order to ensure that abuse of a service medium by a third party is more surely prevented, since such method is suggested by Odagawa '949(see paragraph 205).

Regarding claim 17, Labaton'684 discloses, wherein the first device is further configured to transmit the first and second message modification key values to the second device (column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key).

Regarding claim 18, Labaton'684 discloses, wherein the first and second modified data messages are both transmitted via a first communication channel (fig 1, transmission line 24, the encrypted data is transmitted via transmission line 24).

Regarding claim 21, Labaton'684 discloses, a method for transmitting data over a computer network to a predetermined recipient (see Fig 1, i.e. transmitting bank card information from special tone dialer unit 16 to the host computer 28), the method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message(see column 5, lines 10-13, notice, the card information is encrypted using the current time(GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter(see column 5, lines 10-13, Greenwich Mean Time(GMT));

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (see column 6, lines 59-67, encrypting the next message using changing GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (see column 6, lines 59-67, i.e. the time changes every second, and this changing time is used for encryption);

transmitting the first and second modified data messages to a first device(see Fig.1, i.e. transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28);determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value (see column 6 lines 34-40, i.e. the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key);

and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value(see column 6 lines 34-40, i.e. the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (see column 6, line 60 - column 7 line 5, i.e. the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute with the same encryption key (GMT));

Labaton ’684 does not explicitly teach, wherein the first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient.

Odagawa ‘949 teaches, wherein the first message modification key value being determined based on the at least one variable parameter (see paragraphs 126, 204, Figs. 2 and 7, i.e. using variable information from a variable information provider 47 to generate encryption key 43) and a unique identifier identifying the predetermined recipient(see paragraphs 205-207, 210, Figs. 2 and 7, i.e. information receiver 61 receiving , encrypted information 66, which is encrypted using variable information from variable information provider and biometrics information from a receiving user), the unique identifier being a biometric identifier obtained from the recipient(see paragraphs, 205, 210 and Fig. 2, i.e. a biometric information from a service receiving user is used to generate encryption keys).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using variable information and biometrics information for generating an encryption key as taught by Odagawa ‘949, into the communication system of Labaton ’684, in order to ensure that abuse of a service medium by a third party is more surely prevented, since such method is suggested by Odagawa ‘949(see paragraph 205).

4. **Claims 8-10, 19 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton’684 and Odagawa ‘949 as applied to **claims 1 and 11** above, and further in view of Kamperman et al(US 2002/0004903 A1).

Regarding claim 8, Labaton’684 and Odagawa ‘949 failed to teach, wherein the first and second message modification key values are both transmitted via a second communication channel.

However, Kamperman'903 teaches, wherein the first and second message modification key values are both transmitted via a second communication channel (see paragraph 9, notice, kamperman’903 teaches, method of transmitting the encryption key and the encrypted data separately).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encryption key and encrypted data on a separate channel as taught by Kamperman'903 in to the STD 16 of Labaton’684, in order to send the encryption key quicker, so that in the receiving device all key codes for decryption and accessing the content is already available, since such a method is suggested by Kamperman'903(paragraph 9).

Regarding claim 9, Labaton'684 and Odagawa '949 failed to teach, wherein said first data message comprises voice data.

However, Kamperman'903 teaches, wherein said first data message comprises voice data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

Regarding claim 10, Labaton'684 and Odagawa '949 failed to teach, wherein said first data message comprises video data.

However, Kamperman'903 teaches, wherein said first data message comprises video data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton’684, for controlled distribution of digital information, since such a method is suggested by Kampeman’903(paragraph 9).

Regarding claim 19, Labaton’684 and Odagawa ‘949 failed to teach, wherein said first data message comprises voice data.

However, Kamperman'903 teaches, wherein said first data message comprises voice data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton’684, for controlled distribution of digital information, since such a method is suggested by Kampeman’903(paragraph 9).

Regarding claim 20, Labaton’684 and Odagawa ‘949 failed to teach, wherein said first data message comprises video data.

However, Kamperman'903 teaches, wherein said first data message comprises video data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

(10) Response to Argument

<u>Claims 1-4, 6-15 and 17-21</u>

Regarding Claims 1-4, 6,7,11-15, 17, 18 and 21 the appellant argues that…

(I) Labaton discusses a PIN that is used by the sender of a message to encrypt a transmission. However, *Labaton fails to teach a unique identifier identifying the recipient used in modifying the message*. The PIN in Labaton is not related to a predetermined recipient, but rather is related to the sender of the message… As noted by the Examiner, Labaton *fails to teach a unique identifier associated with the predetermined recipient used as part of a first message modification key value…* page 5 paragraphs 3 and 4.

(II) The Examiner relies on Odagawa as allegedly teaching "a first message modification key value being determined based on the at least one variable parameter and a unique identifier identifying the predetermined recipient, the unique identifier being a biometric identifier obtained from the recipient." Applicant respectfully disagrees with this interpretation of Odagawa… page 5 paragraph 4.

(III) In Odagawa the biometrics information is not used as a message modification key. The biometrics information in Odagawa is the information being modified by the encryption key. The biometric information is not used to determine a first message modification key value as recited in claim 1. Rather, the biometric information in Odagawa is the information that is modified by the encryption key. Thus, the combination of Labaton and Odagawa fails to teach the elements of claim 1… page 6 paragraph 1.

(IV) It is not clear how the Examiner proposes combining Labaton and Odagawa. Labaton relates to a messaging system that encrypts confidential data using a variable (e.g., time). Odagawa teaches encrypting variable information and biometric information to authenticate a user. To arrive at claim 1, one would need to use the biometric information in Odagawa as part of the encryption process in Labaton. This combination is flawed for multiple reasons. First, there is no teaching in Odagawa of using biometric information to encrypt other information. The biometric information is encrypted and used to authenticate a requester. Second, the sender in Labaton would need to have the recipient's biometric information in order to use it for encrypting a message… page 6 and 7.

In response to appellant arguments, examiner respectfully disagrees with the argument above.

(I) In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., *a unique identifier <u>identifying the recipient used in modifying the message</u>, a unique identifier <u>associated with the predetermined recipient</u> used as part of a first message modification key value)* are not recited in the rejected claim(s*)*. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Appellant does **<u>not</u>** specifically claimed, *a unique identifier <u>identifying the recipient used in modifying the message,</u> a unique identifier <u>associated with the predetermined recipient</u> used as part of a first message modification key value.*

(II) Odagawa teaches, wherein the first message modification key value being determined based on the at least one variable parameter (see paragraphs 126, 204, Figs. 2 and 7, i.e. using variable information from a variable information provider 47 to generate encryption key 43), and a unique identifier identifying the predetermined recipient(see paragraphs 205-207, 210, Figs. 2 and 7, i.e., Odagawa suggested that, using biometric information of a user to encrypt the encrypted information 66 ensures prevention of a third party from abusing a service medium, notice, examiner interprets appellants *"unique identifier identifying the predetermined recipient"* as Odagawa's *"biometric information of a user"* used to encrypt encrypted information 66), the unique identifier being a biometric identifier obtained from the recipient(see paragraphs, 205, 210 and Fig. 2, i.e. Odagawa suggest, using biometric information to encrypt and decode, encrypted information 66).

Furthermore Odagawa teaches, requiring information receiver/ service medium purchasers biometric information in order to decode stored encrypted information in the service medium, wherein the stored encrypted information is, encrypted using the purchasers biometric information (see paragraphs 204, 205, 209 ,210 and Fig. 7, i.e. using biometric information 43 in order to decode encrypted information 66), thus Odagawa teaches appellant's argued limitations.

(III) In response to appellant's argument above, the rejection is based upon a combined system of Labaton and Odagawa. One must consider the combined system of Labaton and Odagawa as **a whole,** rather than individually as incorrectly stated by appellant above. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the Examiner has outlined how the combination of the references, when considered as a whole, read on the present claimed invention as follows:

Labaton teaches, a method for transmitting data over a computer network to a predetermined recipient (see Fig 1, i.e. transmitting bank card information from special tone dialer(STD) unit 16 to the host computer 28), the method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message(see column 5, lines 10-13, i.e. the card information is encrypted using the current time(GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter(see column 5, lines 10-13, i.e. Greenwich Mean Time(GMT));

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (see column 6, lines 59-67, i.e. encrypting the next message using the changing GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (see column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

transmitting the first and second modified data messages to a first device(see Fig.1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28);determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving interface computer 26 in order to use it as a decryption key);

and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value(see column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (see column 6, line 60 - column 7 line 5, i.e. the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute using the same encryption key (GMT));

Labaton also teaches, wherein the first message modification key value being determined based on the at least one variable parameter (column 5, lines 10-13 and column 6, line 60 - column 7 line 5, i.e. encrypting a bank card information using current time (GMT), as an encryption key),

Odagawa teaches, wherein the first message modification key value being determined based on the at least one variable parameter (see paragraphs 126, 204, Figs. 2 and 7, i.e. using variable information from a variable information provider 47 to generate encryption key 43), and a unique identifier identifying the predetermined recipient(see paragraphs 205-207, 210, Figs. 2 and 7, i.e., Odagawa suggested that, using biometric information of a user to encrypt the encrypted information 66 ensures prevention of a third party from abusing a service medium, notice, examiner interprets appellants *"unique identifier identifying the predetermined recipient" "biometric information of a user"* used to encrypt encrypted information 66) the unique identifier being a biometric identifier obtained from the recipient(see paragraphs, 205, 210 and Fig. 2, i.e. Odagawa suggests, using biometric information to encrypt and decode, encrypted information 66).

(IV) In response to appellant's argument above, the combination of Labaton and Odagawa is proper as set forth in above response. Also, noted that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In this case, appellant agreement is based on bodily incorporation of Odagawa with Labaton, where the rejection is based on what the combined teachings of the references would have suggested to those of ordinary skill in the art. Thus, it is clear that the combination is appropriate and proper.

Thus, it is clear that the combined system of Labaton and Odagawa disclosed appellant's broadly claimed invention.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/AWET HAILE/
Examiner, Art Unit 2416

/Aung S. Moe/
Supervisory Patent Examiner, Art Unit 2416

/KWANG B. YAO/
Supervisory Patent Examiner, Art Unit 2416